

National Cyber Alert System

[Archive](#)

Cyber Security Bulletin SB09-194

Vulnerability Summary for the Week of July 6, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities					
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info	
apple -- iphone_os	Unspecified vulnerability in Apple iPhone OS allows remote attackers to execute arbitrary code, obtain GPS coordinates, or enable the microphone via an SMS message, as demonstrated by Charlie Miller at SyScan '09 Singapore.	2009-07-05	10.0	CVE-2009-2315 MISC MISC	
apple -- safari	WebKit in Apple Safari before 4.0.2 does not properly handle numeric character references, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted HTML document.	2009-07-09	9.3	CVE-2009-1725 BID CONFIRM APPLE	
awingsoft -- awakening_winds3d_viewer_plugin	Insecure method vulnerability in Awingsoft Awakening Winds3D Viewer plugin 3.5.0.0, 3.0.0.5, and possibly other versions allows remote attackers to force the download and execution of arbitrary files via the GetURL method.	2009-07-10	7.5	CVE-2009-2386 VUPEN BID MISC SECUNIA	
axesstel -- mv_410r	The Axesstel MV 410R has a certain default administrator password, and does not force a password change, which makes it easier for remote attackers to obtain access.	2009-07-05	10.0	CVE-2009-2317 BID BUGTRAQ	
	The Axesstel MV 410R allows remote attackers to	2009-07-		CVE-2009-2319	

axesstel -- mv_410r	cause a denial of service via a flood of SYN packets, a related issue to CVE-1999-0116.	2009-07-05	7.8	CVE-2009-2310 BID BUGTRAQ
axesstel -- mv_410r	The web interface on the Axessel MV 410R relies on client-side JavaScript code to validate input, which allows remote attackers to send crafted data, and possibly have unspecified other impact, via a client that does not process JavaScript.	2009-07-05	7.5	CVE-2009-2320 BID BUGTRAQ
blogtrafficexchange -- related-sites	SQL injection vulnerability in BTE_RW_webajax.php in the Related Sites plugin 2.1 for WordPress allows remote attackers to execute arbitrary SQL commands via the guid parameter.	2009-07-08	7.5	CVE-2009-2383 XF BID
clansphere -- clansphere	Multiple SQL injection vulnerabilities in ClanSphere before 2009.0.1 allow remote attackers to execute arbitrary SQL commands via unknown parameters to the gbook module and unspecified other components.	2009-07-07	7.5	CVE-2009-2345 VUPEN BID
dan_cahill -- nullogic_groupware	Multiple stack-based buffer overflows in the pgsqlQuery function in NullLogic Groupware 1.2.7, when PostgreSQL is used, might allow remote attackers to execute arbitrary code via input to the (1) POP3, (2) SMTP, or (3) web component that triggers a long SQL query.	2009-07-07	9.3	CVE-2009-2356 BUGTRAQ
datachecknh -- gallerypal_fe	SQL injection vulnerability in login.asp in DataCheck Solutions GalleryPal FE 1.5 allows remote attackers to execute arbitrary SQL commands via unspecified vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-07-08	7.5	CVE-2009-2365 XF OSVDB SECUNIA
datachecknh -- forumpal datachecknh -- forumpal_fe	SQL injection vulnerability in login.asp in DataCheck Solutions ForumPal FE 1.1 and ForumPal 1.5 allows remote attackers to execute arbitrary SQL commands via the (1) password parameter in 1.1 and (2) p_password parameter in 1.5. NOTE: some of these details are obtained from third party information.	2009-07-08	7.5	CVE-2009-2366 XF OSVDB OSVDB MILWoRM SECUNIA SECUNIA
david_hansson -- ruby_on_rails	The example code for the digest authentication functionality (http_authentication.rb) in Ruby on Rails before 2.3.3 defines an authenticate_or_request_with_http_digest block that returns nil instead of false when the user does not exist, which allows context-dependent attackers to bypass authentication for applications that are derived from this example by sending an invalid username without a password.	2009-07-10	7.5	CVE-2009-2422 XF VUPEN BID CONFIRM MISC
dutchmonkey -- dm_album	PHP remote file inclusion vulnerability in template/album.php in DM Albums 1.9.2, as used standalone or as a WordPress plugin, allows remote attackers to execute arbitrary PHP code via a URL in the SECURITY_FILE parameter.	2009-07-09	9.3	CVE-2009-2396 BID SECUNIA
ebayclonescript -- ebay_clone	SQL injection vulnerability in category.php in Ebay Clone 2009 allows remote attackers to execute arbitrary SQL commands via the cate_id parameter in a list action.	2009-07-10	7.5	CVE-2009-2423 SECUNIA MISC
f_simea_in_com_bookflip	SQL injection vulnerability in the BookFlip (com_bookflip) component 2.1 for Joomla! allows	2009-07-11	7.5	CVE-2009-2390 BID

i-cmag-mi -- com_bookmark	remote attackers to execute arbitrary SQL commands via the book_id parameter to index.php.	09	7.5	BID MILWORM SECUNIA
fckeditor -- fckeditor	Multiple directory traversal vulnerabilities in FCKeditor before 2.6.4.1 allow remote attackers to create executable files in arbitrary directories via directory traversal sequences in the input to unspecified connector modules, as exploited in the wild for remote code execution in July 2009, related to the file browser and the editor/filemanager/connectors/ directory.	2009-07-05	7.5	CVE-2009-2265 MISC
fijiwebdesign -- com_php	SQL injection vulnerability in the PHP (com_php) component for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter to index.php.	2009-07-09	7.5	CVE-2009-2400 VUPEN
fustrate -- member_awards	SQL injection vulnerability in the awardsMembers function in Sources/Profile.php in the Member Awards component 1.0.2 for Simple Machines Forum (SMF) allows remote attackers to execute arbitrary SQL commands via the id parameter in a profile action to index.php. NOTE: some of these details are obtained from third party information.	2009-07-08	7.5	CVE-2009-2385 XF BID SECUNIA
iomega -- storcenter_pro	cgi-bin/makecgi-pro in Iomega StorCenter Pro generates predictable session IDs, which allows remote attackers to hijack active sessions and gain privileges via brute force guessing attacks on the session_id parameter.	2009-07-08	7.5	CVE-2009-2367 XF MISC SECUNIA OSVDB
jay-jayxor -- phpmyblockchecker	admin.php in phpMyBlockchecker 1.0.0055 allows remote attackers to bypass authentication and gain administrative access by setting the PHPMYBCAdmin cookie to LOGGEDIN.	2009-07-08	7.5	CVE-2009-2382 XF MILWORM SECUNIA OSVDB
joomla -- joomla! markus_donhauser -- ice_gallery_component_for_joomla	SQL injection vulnerability in the Ice Gallery (com_ice) component 0.5 beta 2 for Joomla! allows remote attackers to execute arbitrary SQL commands via the catid parameter to index.php.	2009-07-07	7.5	CVE-2008-6852 XF BID MILWORM
joomlaworks -- com_k2	SQL injection vulnerability in the K2 (com_k2) component 1.0.1 Beta and earlier for Joomla! allows remote attackers to execute arbitrary SQL commands via the category parameter in an itemlist action to index.php.	2009-07-09	7.5	CVE-2009-2395 VUPEN BID MILWORM
jtr -- jax_formmailer	PHP remote file inclusion vulnerability in formmailer.admin.inc.php in Jax FormMailer 3.0.0 allows remote attackers to execute arbitrary PHP code via a URL in the BASE_DIR[jax_formmailer] parameter.	2009-07-08	7.5	CVE-2009-2378 XF
jun_furuse -- camlimages	Multiple integer overflows in CamlImages 2.2 and earlier might allow context-dependent attackers to execute arbitrary code via a crafted PNG image with large width and height values that trigger a heap-based buffer overflow in the (1) read_png_file or (2) read_png_file_as_rgb24 function.	2009-07-05	7.5	CVE-2009-2295 BUGTRAQ MISC
	Buffer overflow in amp.exe in Brothersoft PEamp 1.02b allows user-assisted remote attackers to execute	2009-07-07		CVE-2009-2384

mathi -- peamp	arbitrary code via a long string in a .m3u playlist file. NOTE: some of these details are obtained from third party information.	2009-07-08	9.3	XF MILWORM SECUNIA
matteo_ricchetti -- ss5	Unspecified vulnerability in Socks Server 5 before 3.7.8-8 has unknown impact and attack vectors.	2009-07-08	10.0	CVE-2009-2368 VUPEN CONFIRM SECUNIA
max_kervin -- kervinet_forum	SQL injection vulnerability in topic.php in KerviNet Forum 1.1 allows remote attackers to execute arbitrary SQL commands via the forum parameter.	2009-07-05	7.5	CVE-2007-6727 MISC
microsoft -- windows_2003_server microsoft -- windows_xp	Stack-based buffer overflow in MPEG2TuneRequest in the Microsoft Video ActiveX control in msvidctl.dll in Microsoft DirectShow in Windows 2000, XP, and Server 2003 allows remote attackers to execute arbitrary code via a crafted web page, as exploited in the wild in July 2009.	2009-07-07	9.3	CVE-2008-0015 BID CONFIRM ISS MISC MISC
microsoft -- windows_2003_server microsoft -- windows_xp	Unspecified vulnerability in the Microsoft Video ActiveX control in msvidctl.dll allows remote attackers to execute arbitrary code via unknown vectors that trigger memory corruption, a different vulnerability than CVE-2008-0015.	2009-07-07	9.3	CVE-2008-0020 ISS
mp3-nator -- mp3-nator	Stack-based buffer overflow in Mp3-Nator 2.0 allows remote attackers to execute arbitrary code via a long string in a .plf file, possibly related to a track entry.	2009-07-08	9.3	CVE-2009-2364 XF VUPEN
netcat -- netcat	SQL injection vulnerability in modules/poll/index.php in AIST NetCat 3.0 and 3.12 allows remote attackers to execute arbitrary SQL commands via the PollID parameter.	2009-07-07	7.5	CVE-2008-6853 XF BID MILWORM
nulllogic -- groupware	SQL injection vulnerability in the auth_checkpass function in the login page in NullLogic Groupware 1.2.7 allows remote attackers to execute arbitrary SQL commands via the username parameter.	2009-07-07	7.5	CVE-2009-2354 BUGTRAQ
ocsinventory-ng -- ocs_inventory_ng ocsinventory-ng -- ocsinventory-agent	Untrusted search path vulnerability in Agent/Backend.pm in Ocsinventory-Agent before 0.0.9.3, and 1.x before 1.0.1, in OCS Inventory allows local users to gain privileges via a Trojan horse Perl module in an arbitrary directory.	2009-07-09	7.2	CVE-2009-0667 VUPEN BID CONFIRM DEBIAN CONFIRM CONFIRM CONFIRM
opial -- opial	SQL injection vulnerability in admin/index.php in Opial 1.0 allows remote attackers to execute arbitrary SQL commands via the txtUserName (aka User Name) parameter. NOTE: some of these details are obtained from third party information.	2009-07-07	7.5	CVE-2009-2340 BID MILWORM SECUNIA OSVDB
osTicket -- osTicket	SQL injection vulnerability in include/class.staff.php in osTicket before 1.6 RC5 allows remote attackers to	2009-07- -	-	CVE-2009-2361 XF VUPEN SECTRACK

osTicket -- osTicket	execute arbitrary SQL commands via the staff username parameter.	08	7.5	BUGTRAQ OSVDB MISC SECUNIA CONFIRM
photo-dvd-maker -- photo_dvd_maker	Stack-based buffer overflow in Photo DVD Maker 8.02, and possibly earlier versions, allows remote attackers to execute arbitrary code via a long File_Name parameter in a .pdm file. NOTE: some of these details are obtained from third party information.	2009-07-08	9.3	CVE-2009-2375 VUPEN BUGTRAQ SECUNIA MISC
phpecho_cms -- phpecho_cms	SQL injection vulnerability in index.php in the forum module in PHPEcho CMS 2.0-rc3 allows remote attackers to execute arbitrary SQL commands via the id parameter in a thread action, a different vector than CVE-2008-0355.	2009-07-09	7.5	CVE-2009-2402 BID MILWoRM
rentventory -- rentventory	SQL injection vulnerability in index.php in Rentventory allows remote attackers to execute arbitrary SQL commands via the product parameter.	2009-07-07	7.5	CVE-2009-2339 MILWoRM SECUNIA OSVDB
shalwan -- opial	SQL injection vulnerability in albumdetail.php in Opial 1.0 allows remote attackers to execute arbitrary SQL commands via the albumid parameter.	2009-07-07	7.5	CVE-2009-2341 BID MILWoRM SECUNIA OSVDB
shinji-chiba -- scmpx	Heap-based buffer overflow in SCMPX 1.5.1 allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via a long string in a .m3u playlist file.	2009-07-09	9.3	CVE-2009-2403 VUPEN SECUNIA
smspages -- smspages	SQL injection vulnerability in cat.php in SMSPages 1.0 in Mr.Saphp Arabic Script Mobile (aka Messages Library) 2.0 allows remote attackers to execute arbitrary SQL commands via the CatID parameter.	2009-07-09	7.5	CVE-2009-2394
sourcefire -- 3d_sensor sourcefire -- defense_center	The web-based management interfaces in Sourcefire Defense Center (DC) and 3D Sensor before 4.8.2 allow remote authenticated users to gain privileges via a \$admin value for the admin parameter in an edit action to admin/user/user.cgi and unspecified other components.	2009-07-07	9.0	CVE-2009-2344 VUPEN SECTRACK BID BUGTRAQ MILWoRM SECUNIA
virtuenetz -- virtue_online_test_generator	SQL injection vulnerability in text.php in Virtuenetz Virtue Online Test Generator allows remote attackers to execute arbitrary SQL commands via the tid parameter.	2009-07-09	7.5	CVE-2009-2392 XF
yasinkaplan -- tekradius	The default configuration of TekRADIUS 3.0 uses the sa account to communicate with Microsoft SQL Server, which makes it easier for remote attackers to obtain privileged access to the database and the underlying Windows operating system.	2009-07-07	10.0	CVE-2009-2357 BUGTRAQ
yasinkaplan -- tekradius	Multiple SQL injection vulnerabilities in TekRADIUS 3.0 allow context-dependent attackers to execute arbitrary SQL commands via (1) the GUI client, as demonstrated by input to the Browse Users text box	2009-07-07	7.5	CVE-2009-2359 BUGTRAQ

	in the Users tab; or (2) the command-line client, as demonstrated by a certain trcli -r command.		BUGTRAQ
yukudr -- audioplus	Stack-based buffer overflow in KUDRSOFT AudioPLUS 2.0.0.215 allows remote attackers to execute arbitrary code via a long string in a (1) .lst or (2) .m3u playlist file.	2009-07-08	9.3 CVE-2009-2362 XF VUPEN MILWoRM SECUNIA MISC OSVDB
yukudr -- audioplus	Stack-based buffer overflow in KUDRSOFT AudioPLUS 2.00.215 allows remote attackers to execute arbitrary code via a .pls playlist file with a playlist entry containing a long File1 argument.	2009-07-08	9.3 CVE-2009-2363 XF MILWoRM MISC

[Back to top](#)**Medium Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The forum module in NullLogic Groupware 1.2.7 allows remote authenticated users to cause a denial of service (application crash) by specifying (1) an empty string or (2) a non-numeric string when selecting a forum, related to the fmessagelist function.	2009-07-07	4.0	CVE-2009-2355 BUGTRAQ
4homepages -- 4images	Cross-site scripting (XSS) vulnerability in includes/functions.php in 4images 1.7 through 1.7.7 allows remote attackers to inject arbitrary web script or HTML via vectors related to the url variable.	2009-07-08	4.3	CVE-2009-2380 XF BID OSVDB CONFIRM SECUNIA
apache -- http_server	The mod_deflate module in Apache httpd 2.2.11 and earlier compresses large files until completion even after the associated network connection is closed, which allows remote attackers to cause a denial of service (CPU consumption).	2009-07-10	4.3	CVE-2009-1891 REDHAT CONFIRM MANDRIVA
apple -- safari	Use-after-free vulnerability in the servePendingRequests function in WebCore in WebKit in Apple Safari 4.0 and 4.0.1 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted HTML document that references a zero-length .js file and the JavaScript reload function. NOTE: some of these details are obtained from third party information.	2009-07-09	4.3	CVE-2009-2419 XF BID OSVDB CONFIRM SECUNIA MISC
apple -- safari	Apple Safari 3.2.3 does not properly implement the file: protocol handler, which allows remote attackers to read arbitrary files or cause a denial of service (launch of multiple Windows Explorer instances) via vectors involving an unspecified HTML tag, possibly a related issue to CVE-2009-1703.	2009-07-09	5.8	CVE-2009-2420 BUGTRAQ
apple -- safari	The CFCharacterSetInitInlineBuffer method in CoreFoundation.dll in Apple Safari 3.2.3 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly execute arbitrary code via a "high-bit character" in a URL	2009-07-09	5.0	CVE-2009-2421 BUGTRAQ

	fragment for an unspecified protocol.			
apple -- safari	Cross-site scripting (XSS) vulnerability in WebKit in Apple Safari before 4.0.2 allows remote attackers to inject arbitrary web script or HTML via vectors related to parent and top objects.	2009-07-09	4.3	CVE-2009-1724 CONFIRM APPLE
audioarticledirectory -- audio_article_directory	Directory traversal vulnerability in download.php in Audio Article Directory allows remote attackers to read arbitrary files via directory traversal sequences in the file parameter.	2009-07-09	5.0	CVE-2009-2397 VUPEN MILWORM SECUNIA
avax-software -- avax_vector_activex	Buffer overflow in the Avax Vector ActiveX control in avPreview.ocx in AVAX-software Avax Vector ActiveX 1.3 allows remote attackers to cause a denial of service (application crash) via a long PrinterName property.	2009-07-08	4.3	CVE-2009-2377 BID BUGTRAQ
bigace -- bigace_cms	Directory traversal vulnerability in public/index.php in BIGACE Web CMS 2.6 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the cmd parameter.	2009-07-08	6.8	CVE-2009-2379 CONFIRM CONFIRM
cms.tut.su -- cms_chainuk	Cross-site scripting (XSS) vulnerability in admin/admin_menu.php in CMS Chainuk 1.2 and earlier allows remote attackers to inject arbitrary web script or HTML via the menu parameter.	2009-07-05	4.3	CVE-2009-2330 MILWORM
drupal -- drupal	Drupal 6.x before 6.13 does not prevent users from modifying user signatures after the associated comment format has been changed to an administrator-controlled input format, which allows remote authenticated users to inject arbitrary web script, HTML, and possibly PHP code via a crafted user signature.	2009-07-08	6.5	CVE-2009-2372 SECTRACK OSVDB CONFIRM
drupal -- drupal	Cross-site scripting (XSS) vulnerability in the Forum module in Drupal 6.x before 6.13 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-07-08	4.3	CVE-2009-2373 CONFIRM
drupal -- drupal	Drupal 5.x before 5.19 and 6.x before 6.13 does not properly sanitize failed login attempts for pages that contain a sortable table, which includes the username and password in links that can be read from (1) the HTTP referer header of external web sites that are visited from those links or (2) when page caching is enabled, the Drupal page cache.	2009-07-08	5.0	CVE-2009-2374 OSVDB CONFIRM
dutchmonkey -- dm_filemanager	PHP remote file inclusion vulnerability in dm-albums/template/album.php in DM FileManager 3.9.4, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the SECURITY_FILE parameter.	2009-07-09	6.8	CVE-2009-2399 SECUNIA
eaccelerator -- eaccelerator	encoder.php in eAccelerator allows remote attackers to execute arbitrary code by copying a local executable file to a location under the web root via the -o option, and then making a direct request to this file, related to upload of image files.	2009-07-07	6.8	CVE-2009-2353 BUGTRAQ
ebayclonescript -- ebay_clone	Cross-site scripting (XSS) vulnerability in search.php in Ebay Clone 2009 allows remote attackers to inject arbitrary web script or HTML via the mode parameter.	2009-07-10	4.3	CVE-2009-2424 SECUNIA MISC
fckeditor -- fckeditor	Multiple cross-site scripting (XSS) vulnerabilities in FCKeditor before 2.6.4.1 allow remote attackers to inject arbitrary web script or HTML via components in the	2009-07-05	4.3	CVE-2009-2324 MISC

	samples (aka _samples) directory.			MISC
freewebshop -- freewebshop	Directory traversal vulnerability in includes/startmodules.inc.php in FreeWebshop.org 2.2.9 R2, when register_globals is enabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the lang_file parameter.	2009-07-07	6.8	CVE-2009-2338 MILWoRM SECUNIA
gizmo5 -- gizmo	Gizmo 3.1.0.79 on Linux does not verify a server's SSL certificate, which allows remote servers to obtain the credentials of arbitrary users via a spoofed certificate.	2009-07-08	5.0	CVE-2009-2381 XF BID BUGTRAQ SECUNIA
google -- chrome	Google Chrome 1.0.154.48 and earlier does not block javascript: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header or (2) specifying the content of a Refresh header, a related issue to CVE-2009-1312.	2009-07-07	4.3	CVE-2009-2352 BID BUGTRAQ BUGTRAQ MISC
hans_oesterholt -- cmme	Cross-site scripting (XSS) vulnerability in admin.php (aka the login page) in Content Management Made Easy (CMME) before 1.22 allows remote attackers to inject arbitrary web script or HTML via the username field.	2009-07-07	4.3	CVE-2009-2342 MISC CONFIRM SECUNIA
horde -- passwd	Cross-site scripting (XSS) vulnerability in passwd/main.php in the Passwd module before 3.1.1 for Horde allows remote attackers to inject arbitrary web script or HTML via the backend parameter.	2009-07-08	4.3	CVE-2009-2360 VUPEN BID MLIST
ibm -- tivoli_identity_manager	Multiple cross-site scripting (XSS) vulnerabilities in IBM Tivoli Identity Manager (ITIM) 5.0 allow remote attackers to inject arbitrary web script or HTML by entering an unspecified URL in (1) the self-service UI interface or (2) the console interface.	2009-07-05	4.3	CVE-2009-2316 CONFIRM
linux -- kernel	The ptrace_start function in kernel/ptrace.c in the Linux kernel 2.6.18 does not properly handle simultaneous execution of the do_coredump function, which allows local users to cause a denial of service (deadlock) via vectors involving the ptrace system call and a coredumping thread.	2009-07-05	4.9	CVE-2009-1388 CONFIRM CONFIRM CONFIRM MLIST
max_kervin -- kervinet_forum	KerviNet Forum 1.1 and earlier allows remote attackers to obtain sensitive information via a direct request to (1) admin/head.php, or (2) voting_diagram.php, (3) voting.php, (4) topics_search.php, (5) topics_list.php, (6) top_part.php, (7) quick_search.php, (8) quick_reply.php, (9) moder_menu.php, (10) messages_list.php, (11) menu.php, (12) head.php, (13) forums_list.php, (14) forum_statistics.php, (15) forum_info.php, or (16) birthday.php in include_files/, which reveals the installation path in an error message.	2009-07-05	5.0	CVE-2009-2329 MILWoRM
michelle_cox -- advanced_forum	Cross-site scripting (XSS) vulnerability in Advanced Forum 5.x before 5.x-1.1 and 6.x before 6.x-1.1, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-07-08	4.3	CVE-2009-2370 VUPEN OSVDB CONFIRM CONFIRM CONFIRM

michelle_cox -- advanced_forum	Advanced Forum 6.x before 6.x-1.1, a module for Drupal, does not prevent users from modifying user signatures after the associated comment format has been changed to an administrator-controlled input format, which allows remote authenticated users to inject arbitrary web script, HTML, and possibly PHP code via a crafted user signature.	2009-07-08	6.5	CVE-2009-2371 VUPEN CONFIRM CONFIRM
microsoft -- internet_explorer	Microsoft Internet Explorer 6.0.2900.2180 and earlier does not block javascript: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header or (2) specifying the content of a Refresh header, a related issue to CVE-2009-1312 .	2009-07-07	4.3	CVE-2009-2350 BID BUGTRAQ BUGTRAQ MISC
microsoft -- ie	Stack-based buffer overflow in the AddFavorite method in Microsoft Internet Explorer allows remote attackers to cause a denial of service (application crash) and possibly have unspecified other impact via a long URL in the first argument.	2009-07-10	4.3	CVE-2009-2433 BID MILWORM
opera -- opera_browser	Opera 9.52 and earlier does not block javascript: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header or (2) specifying the content of a Refresh header, a related issue to CVE-2009-1312 .	2009-07-07	4.3	CVE-2009-2351 BID BUGTRAQ BUGTRAQ MISC
php-fusion -- php-fusion	Cross-site scripting (XSS) vulnerability in messages.php in PHP-Fusion 6.01.17 and 7.00.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-07-07	4.3	CVE-2008-6850 XF BID CONFIRM
php-sugar -- php-sugar	Directory traversal vulnerability in test/index.php in PHP-Sugar 0.80 allows remote attackers to read arbitrary files via a ..// (dot dot slash slash) in the t parameter.	2009-07-09	5.0	CVE-2009-2398 VUPEN
php_link_directory -- php_link_directory	SQL injection vulnerability in page.php in PHP Link Directory (phpLD) 3.3, when register_globals is enabled and magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the name parameter.	2009-07-07	5.1	CVE-2008-6851 XF BID MILWORM
phpecho_cms -- phpecho_cms	Cross-site scripting (XSS) vulnerability in PHPEcho CMS 2.0-rc3 allows remote attackers to inject arbitrary web script or HTML via a forum post.	2009-07-09	4.3	CVE-2009-2401 XF BID MILWORM
shalwan -- opial	SQL injection vulnerability in admin/index.php in Opial 1.0 allows remote attackers to execute arbitrary SQL commands via the txtPassword parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-07-09	6.8	CVE-2009-2388 SECUNIA OSVDB
sun -- opensolaris	Unspecified vulnerability in the proc filesystem in Sun OpenSolaris snv_49 through snv_109 allows local users to cause a denial of service (deadlock and panic) via unknown vectors, related to the ldt_rewrite_syscall function.	2009-07-09	4.9	CVE-2009-2387 SUNALERT
	Cross-site scripting (XSS) vulnerability in the Html::textarea function in			CVE-2009-

tangocms -- tangocms	application/libraries/Html.php in TangoCMS 2.x before 2.3.0 allows remote attackers to inject arbitrary web script or HTML via the value parameter, related to the Contact module.	2009-07-08	4.3	2376 CONFIRM CONFIRM
tor -- tor	Tor before 0.2.0.35 allows remote attackers to cause a denial of service (application crash) via a malformed router descriptor.	2009-07-10	5.0	CVE-2009-2425 XF VUPEN BID OSVDB MLIST
tor -- tor	The connection_edge_process_relay_cell_not_open function in src/or/relay.c in Tor 0.2.x before 0.2.0.35 and 0.1.x before 0.1.2.8-beta allows exit relays to have an unspecified impact by causing controllers to accept DNS responses that redirect to an internal IP address via unknown vectors. NOTE: some of these details are obtained from third party information.	2009-07-10	5.0	CVE-2009-2426 XF VUPEN BID OSVDB MLIST
usolved -- newsolved	Multiple SQL injection vulnerabilities in newsscript.php in USOLVED NEWSolved 1.1.6, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) jahr or (2) idneu parameter in an archive action, or (3) the newsid parameter.	2009-07-09	6.8	CVE-2009-2389 MILWORM SECUNIA
virtuenetz -- virtue_online_test_generator	Cross-site scripting (XSS) vulnerability in text.php in Virtuenetz Virtue Online Test Generator allows remote attackers to inject arbitrary web script or HTML via the tid parameter.	2009-07-09	4.3	CVE-2009-2391 XF MILWORM
virtuenetz -- virtue_online_test_generator	admin/index.php in Virtuenetz Virtue Online Test Generator does not require administrative privileges, which allows remote authenticated users to have an unknown impact via unspecified vectors.	2009-07-09	6.5	CVE-2009-2393 XF MILWORM
w2b -- phpgreetcards	Cross-site scripting (XSS) vulnerability in index.php in phpGreetCards 3.7 allows remote attackers to inject arbitrary web script or HTML via the category parameter in a select action.	2009-07-07	4.3	CVE-2008-6848 XF VUPEN BID MILWORM SECUNIA OSVDB
w2b -- phpgreetcards	Unrestricted file upload vulnerability in index.php in phpGreetCards 3.7 allows remote attackers to execute arbitrary PHP code by uploading a file with an executable extension, then accessing it via a via a link that is listed by userfiles/number_shell.php.	2009-07-07	6.8	CVE-2008-6849 XF VUPEN BID MILWORM SECUNIA OSVDB
w3bcms -- gaestebuch_guestbook_module	SQL injection vulnerability in includes/module/book/index.inc.php in w3b cms Gaestebuch Guestbook Module 3.0.0, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the spam_id parameter.	2009-07-07	6.8	CVE-2009-2337 OSVDB
	Integer overflow in the wxImage::Create function in src/common/image.cpp in wxWidgets 2.8.10 allows attackers to cause a denial of service (crash) and	2009-07-		CVE-2009-2369 XF

wxwidgets -- wxwidgets	possibly execute arbitrary code via a crafted JPEG file, which triggers a heap-based buffer overflow. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-07-08	6.8	VUPEN BID SECUNIA OSVDB
xmb_forum -- xmb	Cross-site scripting (XSS) vulnerability in XMB 1.5 allows remote attackers to inject arbitrary web script or HTML via the MSN field during user registration.	2009-07-05	4.3	CVE-2007-6728 MISC
yasinkaplan -- tekradius	TekRADIUS 3.0 uses BUILTIN\Users:R permissions for the TekRADIUS.ini file, which allows local users to obtain obfuscated database credentials by reading this file.	2009-07-07	4.6	CVE-2009-2358 BUGTRAQ
zoph -- zoph	Cross-site scripting (XSS) vulnerability in people.php in Zoph before 0.7.0.6 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: some of these details are obtained from third party information.	2009-07-07	4.3	CVE-2009-2343 CONFIRM CONFIRM

[Back to top](#)

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sun -- lightweight_availability_collection_tool	Race condition in the Sun Lightweight Availability Collection Tool 3.0 on Solaris 7 through 10 allows local users to overwrite arbitrary files via unspecified vectors.	2009-07-05	2.1	CVE-2009-2314 SUNALERT

[Back to top](#)

Last updated July 13, 2009

 Print This Document